PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-039994
(43)Date of publication of application : 08.02.2000

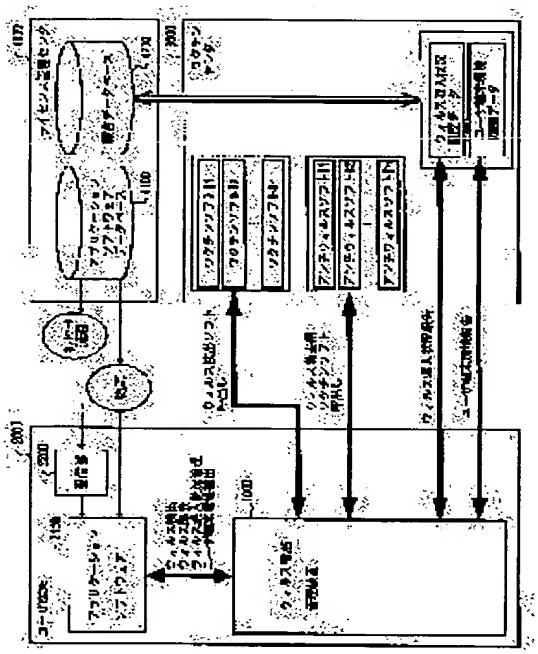
(51)Int.Cl. G06F 9/06

(21)Application number : 10-208245
(22)Date of filing : 23.07.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
SB NETWORKS KK
(72)Inventor : YOSHIKAWA KENICHI
INMAKI NAOFUMI
WAKAI TAKUSANE
SUGANO YUUKI

(54) METHOD AND SYSTEM FOR MANAGING LICENSE WITH VIRUS DETECTION, VACCINE CENTER, AND STORAGE MEDIUM STORED WITH PROGRAM FOR MANAGING LICENSE WITH VIRUS DETECTION

(57)Abstract:
PROBLEM TO BE SOLVED: To quickly detect computer virus by calling virus detection software from a vaccine center which holds the virus detection software, and judging whether or not a digital content is infected by computer virus.
SOLUTION: Plural latest virus detection software is stored in a vaccine center 300. In a user terminal, when a virus detection managing device 1000 is started for operating virus detection check for application software 2100, the virus detection software is requested to a vaccine center 3000. The vaccine center 3000 transmits the requested virus detection software to a user terminal 2000. The user terminal 2000 receives the virus detection software, and stores it in a storage part. Then, whether or not the application software 2100 is infected by virus can be detected by using the stored virus detection software.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－３９９９４
（Ｐ２０００－３９９９４Ａ）
(43)公開日　平成12年2月8日(2000.2.8)

(51)Int.Cl.⁷	識別記号	FI	テーマコード(参考)
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06　５５０　Ｚ	5B076

審査請求　未請求　請求項の数２１　ＯＬ　（全１５頁）

(21)出願番号　特願平10-208245

(22)出願日　平成10年7月23日(1998.7.23)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(71)出願人　598082374
エスビーネットワークス株式会社
東京都中央区日本橋箱崎町24－1

(72)発明者　吉川　研一
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

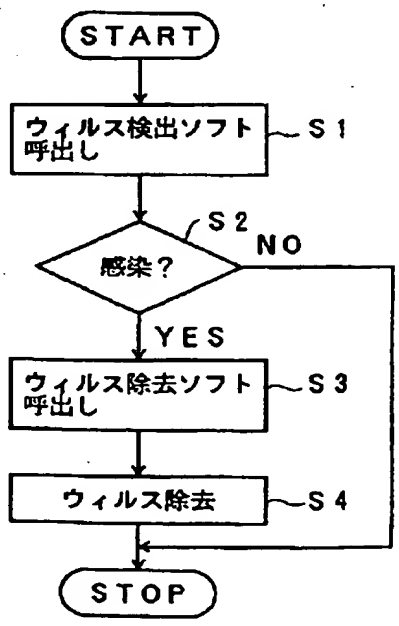
(54)【発明の名称】ウィルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウィルス検出付ライセンス管理プログラムを格納した記憶媒体

(57)【要約】

【課題】　ワクチンセンタに用意されたウィルス検出ソフトとウィルス除去ソフトを呼出し、コンピュータウィルスの検出と除去を行うことが可能なウィルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウィルス検出付ライセンス管理プログラムを格納した記憶媒体を提供する。

【解決手段】　最新のウィルス検出ソフト及びウィルス除去ソフトを保持するワクチンセンタから、該ウィルス検出ソフトを呼出して、ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定し、コンピュータウィルスに感染している場合に、ワクチンセンタからウィルス除去ソフトを呼び出して、ディジタルコンテンツのコンピュータウィルスを除去する。

本発明の原理を説明するための図



1

【特許請求の範囲】

【請求項１】 ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理方法において、

ウィルス検出ソフトを保持するワクチンセンタから、該ウィルス検出ソフトを呼出して、前記ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定することを特徴とするウィルス検出付ライセンス管理方法。

【請求項２】 ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理方法において、

ウィルス除去ソフトを保持するワクチンセンタから、該ウィルス除去ソフトを呼び出して、前記ディジタルコンピュータがコンピュータウィルスに感染している場合に、該ウィルス除去ソフトを用いて該コンピュータウィルスを除去することを特徴とするウィルス検出付ライセンス管理方法。

【請求項３】 ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理方法において、

ウィルス検出ソフト及びウィルス除去ソフトを保持するワクチンセンタから、該ウィルス検出ソフトを呼出して、前記ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定し、

前記コンピュータウィルスに感染している場合に、前記ワクチンセンタから前記ウィルス除去ソフトを呼び出して、前記ディジタルコンテンツの前記コンピュータウィルスを除去することを特徴とするウィルス検出付ライセンス管理方法。

【請求項４】 前記ディジタルコンテンツに関するライセンス使用条件書に、前記コンピュータウィルスの検出結果や除去結果であるウィルス検出日時、ウィルス検出ソフト名、ウィルスの有無、感染したコンピュータウィルスの種類、ウィルス除去日時の何れかを含む履歴データであるウィルス混入状況履歴データを書込み、

前記ウィルス混入状況履歴データを前記ワクチンセンタに送信する請求項３記載のウィルス検出付ライセンス管理方法。

【請求項５】 前記ユーザ端末における使用端末名、端末使用時間、使用コンテンツ名の何れかを含むユーザ端末環境データを抽出し、

前記ユーザ端末環境データを記憶すると共に、前記ワクチンセンタに送信する請求項３乃至４記載のウィルス検出付ライセンス管理方法。

2

【請求項６】 ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムであって、

ウィルス検出ソフトを保持するワクチンセンタと、

前記ワクチンセンタとの通信を行う通信手段と、

前記通信手段により、前記ワクチンセンタから、該ウィルス検出ソフトを呼出して、前記ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出手段とを有するユーザ端末とを有することを特徴とするウィルス検出付ライセンス管理システム。

【請求項７】 ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムであって、

ウィルス除去ソフトを保持するワクチンセンタと、

前記ワクチンセンタとの通信を行う通信手段と、

前記ワクチンセンタから、該ウィルス除去ソフトを呼び出して、前記ディジタルコンピュータがコンピュータウィルスに感染している場合に、該ウィルス除去ソフトを用いて該コンピュータウィルスを除去するウィルス除去手段とを有するユーザ端末とを有することを特徴とするウィルス検出付ライセンス管理システム。

【請求項８】 ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムであって、

ウィルス検出ソフトを保持するウィルス検出ソフト保持手段と、

ウィルス除去ソフトを保持するウィルス除去ソフト保持手段とを有するワクチンセンタと、

前記ワクチンセンタとの通信を行う通信手段と、

前記ワクチンセンタから、該ウィルス検出ソフトを呼出して、前記ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出手段と、

前記ウィルス検出手段において、

前記コンピュータウィルスに感染している場合に、前記ワクチンセンタから前記ウィルス除去ソフトを呼び出して、前記ディジタルコンテンツの前記コンピュータウィルスを除去するウィルス除去手段とを有するユーザ端末とを有することを特徴とするウィルス検出付ライセンス管理システム。

【請求項９】 前記ユーザ端末は、

前記ディジタルコンテンツに関するライセンス使用条件

書に、前記コンピュータウィルスの検出結果や除去結果であるウィルス検出日時、ウィルス検出ソフト名、ウィルスの有無、感染したコンピュータウィルスの種類、ウィルス除去日時の何れかを含む履歴データであるウィルス混入状況履歴データを書込むウィルス混入状況保持手段と、

前記ウィルス混入状況履歴データを前記ワクチンセンタに送信するウィルス混入状況データ送信手段とを有し、

前記ワクチンセンタは、

前記ユーザ端末の前記ウィルス混入状況データ送信手段により送られた前記ウィルス混入状況履歴データを格納するウィルス混入状況データ記憶手段を有する請求項８記載のウィルス検出付ライセンス管理システム。

【請求項１０】　前記ユーザ端末は、

使用端末名、端末使用時間、使用コンテンツ名の何れかを含むユーザ端末環境データを抽出するユーザ端末環境データ抽出手段と、

前記ユーザ端末環境データを記憶するユーザ端末環境データ記憶手段と、

前記ユーザ端末環境データを前記ワクチンセンタに送信する環境データ送信手段とを有する請求項８乃至９記載のウィルス検出付ライセンス管理システム。

【請求項１１】　ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるワクチンセンタであって、

ウィルス検出ソフトを保持するウィルス検出ソフト記憶手段と、

ウィルス除去ソフトを保持するウィルス除去ソフト記憶手段と、

前記ユーザ端末との通信を行う通信手段とを有することを特徴とするワクチンセンタ。

【請求項１２】　前記ユーザ端末から送信されるウィルス混入状況履歴データを格納するウィルス混入状況データ記憶手段を更に有する請求項１１記載のワクチンセンタ。

【請求項１３】　前記ユーザ端末から送信されるユーザ端末環境データを格納するユーザ端末環境データ記憶手段を更に有する請求項１１乃至１２記載のワクチンセンタ。

【請求項１４】　ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるユーザ端末に搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、

前記ワクチンセンタとの通信を行わせる通信プロセスと、

前記通信プロセスにより、前記ワクチンセンタから、該ウィルス検出ソフトを呼出して、前記ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出プロセスとを少なくとも有することを特徴とするウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【請求項１５】　ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるユーザ端末に搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、

前記ワクチンセンタとの通信を行わせる通信プロセスと、

前記ワクチンセンタから、該ウィルス除去ソフトを呼び出して、前記ディジタルコンピュータがコンピュータウィルスに感染している場合に、該ウィルス除去ソフトを用いて該コンピュータウィルスを除去するウィルス除去プロセスとを少なくとも有することを特徴とするウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【請求項１６】　ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるユーザ端末に搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、

前記ワクチンセンタとの通信を行わせる通信プロセスと、

前記ワクチンセンタから、該ウィルス検出ソフトを呼出して、前記ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出プロセスと、

前記ウィルス検出プロセスにおいて、前記コンピュータウィルスに感染している場合に、前記ワクチンセンタから前記ウィルス除去ソフトを呼び出して、前記ディジタルコンテンツの前記コンピュータウィルスを除去するウィルス除去プロセスとを少なくとも有することを特徴とするウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【請求項１７】　前記ディジタルコンテンツに関するライセンス使用条件書に、前記コンピュータウィルスの検出結果や除去結果であるウィルス検出日時、ウィルス検出ソフト名、ウィルスの有無、感染したコンピュータウィルスの種類、ウィルス除去日時の何れかを含む履歴データであるウィルス混入状況履歴データを記憶手段に書込むウィルス混入状況書込プロセスと、

前記ウィルス混入状況履歴データを前記ワクチンセンタ

に送信させるウィルス混入状況データ送信プロセスとをさらに有する請求項１６記載のウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【請求項１８】　使用端末名、端末使用時間、使用コンテンツ名の何れかを含むユーザ端末環境データを抽出するユーザ端末環境データ抽出プロセスと、

前記ユーザ端末環境データを記憶手段に記憶させるユーザ端末環境データ格納プロセスと、

前記ユーザ端末環境データを前記ワクチンセンタに送信させる環境データ送信プロセスとを更に有する請求項１６乃至１７記載のウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【請求項１９】　ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるワクチンセンタに搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、

保持しているウィルス検出ソフトを前記ユーザ端末の要求に基づいて送信させるウィルス検出ソフト送信プロセスと、

保持しているウィルス除去ソフトを前記ユーザ端末の要求に基づいて送信するウィルス除去ソフト送信プロセスとを有することを特徴とするウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【請求項２０】　前記ユーザ端末から送信されたウィルス混入状況履歴データを記憶手段に格納するウィルス混入状況データ格納プロセスを更に有する請求項１９記載のウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【請求項２１】　前記ユーザ端末から送信されるユーザ端末環境データを記憶手段に格納するユーザ端末環境データ格納プロセスを更に有する請求項１９乃至２０記載のウィルス検出付ライセンス管理プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ウィルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウィルス検出付ライセンス管理プログラムを格納した記憶媒体に係り、特に、ゲームソフトを含むコンピュータアプリケーションソフトウェアや、ビデオ、アニメーション、コンピュータグラフィック、モーションキャプチャ等のデジタルデータや、電子スチル写真等のデジタル静止画や、電子音楽、ＭＩＤＩ等のデジタルデータ等のデジタルコンテンツを使用許諾等のライセンスで管理するシステムに対して、デジタルコンテンツに潜入しているコンピュータウィルスを検出・除去し、また、デジタルコンピュータのウィルス混入状況やユーザ端末環境のデータを管理することによってウィルス伝搬状況の把握や、コンピュータウィルス感染の予防を行うウィルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウィルス検出付ライセンス管理プログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】従来におけるデジタルコンピュータのライセンス管理を行う方法としては、例えば、特願平９－２４７２７２号に開示されてる方法がある。当該方法は、ディジタルコンピュータとそのライセンス使用条件書のペア構造を実現するためにリンク処理プログラムであるライセンス管理代理処理装置を実装したシステムにより実現される。

【０００３】

【発明が解決しようとする課題】しかしながら、多種多様化した、コンピュータソフトウェアや文書ファイル等のディジタルコンテンツをライセンス管理するシステムにおいて、端末の使用走行環境がユーザ別に異なっているため、ライセンス管理をしているディジタルコンテンツのウィルス検出が大きな問題となっている。具体的な問題を以下に示す。

【０００４】第１には、コンピュータウィルスが絶えず進化し、また、そのスピードが速いため、ユーザが持っているワクチン系ソフトが対応しきれず、当該コンピュータウィルスを検出できないという問題がある。第２には、コンピュータウィルスがプログラムソフトウェアや文書に複雑に潜入し（マクロウィルス等）、それを除去するためのアンチウィルス系ソフトが極端に増大し、タイムリーに当該アンチウィルス系ソフトを配布できないことから、迅速に除去できないという問題がある。

【０００５】第３には、インターネット等によるネットワーク環境が多岐にわたるため、ライセンス管理しているディジタルコンテンツに関するウィルスの伝搬状況を把握しにくいという問題がある。第４には、ワクチンセンタ側でユーザ個々のディジタルコンピュータ上の走行中のソフトウェア及びハードウェア使用状況等を把握できないと共に、感染したソフトウェアやハードウェアの使用環境や設置場所等を特定しずらいため、ウィルス感染の傾向や状況が把握できず、端末内のウィルス感染の予防対策を立てにくいという問題がある。

【０００６】本発明は、上記の点に鑑みなされたもので、ワクチンセンタに用意されたウィルス検出ソフトとウィルス除去ソフトを呼出し、コンピュータウィルスの検出と除去を行うことが可能なウィルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウィルス検出付ライセンス管理プログラムを格納した記憶媒体を提供することを目的とする。

【０００７】また、本発明の目的は、ディジタルコンテンツに関するライセンス使用条件書に記したウィルス混入状況の履歴データを管理することによって、コンピュ

ータウィルス伝搬状況を把握できるウィルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウィルス検出付ライセンス管理プログラムを格納した記憶媒体を提供することである。

【０００８】更なる本発明の目的は、ユーザ端末の環境データを管理することによって、コンピュータウィルス感染の予防を行うことが可能なウィルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウィルス検出付ライセンス管理プログラムを格納した記憶媒体を提供することである。

【０００９】

【課題を解決するための手段】本発明（請求項１）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理方法において、ウィルス検出ソフトを保持するワクチンセンタから、該ウィルス検出ソフトを呼出して、ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定する。

【００１０】本発明（請求項２）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理方法において、ウィルス除去ソフトを保持するワクチンセンタから、該ウィルス除去ソフトを呼び出して、ディジタルコンピュータがコンピュータウィルスに感染している場合に、該ウィルス除去ソフトを用いて該コンピュータウィルスを除去する。

【００１１】図１は、本発明の原理を説明するための図である。本発明（請求項３）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理方法において、ウィルス検出ソフト及びウィルス除去ソフトを保持するワクチンセンタから、該ウィルス検出ソフトを呼出して（ステップ１）、ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定し（ステップ２）、コンピュータウィルスに感染している場合に、ワクチンセンタからウィルス除去ソフトを呼び出して（ステップ３）、ディジタルコンテンツのコンピュータウィルスを除去する（ステップ４）。

【００１２】本発明（請求項４）は、ディジタルコンテンツに関するライセンス使用条件書に、コンピュータウィルスの検出結果や除去結果であるウィルス検出日時、ウィルス検出ソフト名、ウィルスの有無、感染したコンピュータウィルスの種類、ウィルス除去日時の何れかを含む履歴データであるウィルス混入状況履歴データを書込み、ウィルス混入状況履歴データをワクチンセンタに送信する。

【００１３】本発明（請求項５）は、ユーザ端末における使用端末名、端末使用時間、使用コンテンツ名の何れかを含むユーザ端末環境データを抽出し、ユーザ端末環境データを記憶すると共に、ワクチンセンタに送信する。本発明（請求項６）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムであって、ウィルス検出ソフトを保持するワクチンセンタと、ワクチンセンタとの通信を行う通信手段と、通信手段により、ワクチンセンタから、該ウィルス検出ソフトを呼出して、ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出手段とを有するユーザ端末とを有する。

【００１４】本発明（請求項７）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムであって、ウィルス除去ソフトを保持するワクチンセンタと、ワクチンセンタとの通信を行う通信手段と、ワクチンセンタから、該ウィルス除去ソフトを呼び出して、ディジタルコンピュータがコンピュータウィルスに感染している場合に、該ウィルス除去ソフトを用いて該コンピュータウィルスを除去するウィルス除去手段とを有するユーザ端末とを有する。

【００１５】図２は、本発明の原理構成図である。本発明（請求項８）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムであって、ウィルス検出ソフトを保持するウィルス検出ソフト保持手段１１と、ウィルス除去ソフトを保持するウィルス除去ソフト保持手段１２とを有するワクチンセンタ１０と、ワクチンセンタ１０との通信を行う通信手段２１と、ワクチンセンタ１０から、該ウィルス検出ソフトを呼出して、ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出手段２２と、ウィルス検出手段２２において、コンピュータウィルスに感染している場合に、ワクチンセンタからウィルス除去ソフトを呼び出して、ディジタルコンテンツのコンピュータウィルスを除去するウィルス除去手段２３とを有するユーザ端末２０とを有する。

【００１６】本発明（請求項９）は、ユーザ端末２０において、ディジタルコンテンツに関するライセンス使用条件書に、コンピュータウィルスの検出結果や除去結果であるウィルス検出日時、ウィルス検出ソフト名、ウィ

ルスの有無、感染したコンピュータウィルスの種類、ウィルス除去日時の何れかを含む履歴データであるウィルス混入状況履歴データを書込むウィルス混入状況保持手段と、ウィルス混入状況履歴データをワクチンセンタに送信するウィルス混入状況データ送信手段とを有し、ワクチンセンタ１０において、ユーザ端末のウィルス混入状況データ送信手段により送られたウィルス混入状況履歴データを格納するウィルス混入状況データ記憶手段を有する。

【００１７】本発明（請求項１０）は、ユーザ端末２０において、使用端末名、端末使用時間、使用コンテンツ名の何れかを含むユーザ端末環境データを抽出するユーザ端末環境データ抽出手段と、ユーザ端末環境データを記憶するユーザ端末環境データ記憶手段と、ユーザ端末環境データをワクチンセンタに送信する環境データ送信手段とを有する。

【００１８】本発明（請求項１１）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるワクチンセンタであって、ウィルス検出ソフトを保持するウィルス検出ソフト記憶手段と、ウィルス除去ソフトを保持するウィルス除去ソフト記憶手段と、ユーザ端末との通信を行う通信手段とを有する。

【００１９】本発明（請求項１２）は、ユーザ端末から送信されるウィルス混入状況履歴データを格納するウィルス混入状況データ記憶手段を更に有する。本発明（請求項１３）は、ユーザ端末から送信されるユーザ端末環境データを格納するユーザ端末環境データ記憶手段を更に有する。本発明（請求項１４）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるユーザ端末に搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、ワクチンセンタとの通信を行わせる通信プロセスと、通信プロセスにより、ワクチンセンタから、該ウィルス検出ソフトを呼出して、ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出プロセスとを少なくとも有する。

【００２０】本発明（請求項１５）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるユーザ端末に搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、ワクチンセンタとの通信を行わせる通信プロセスと、ワクチンセンタから、該ウィルス除去ソフトを呼び出して、ディジタルコンピュータがコンピュータウィルスに感染している場合に、該ウィルス除去ソフトを用いて該コンピュータウィルスを除去するウィルス除去プロセスとを少なくとも有する。

【００２１】本発明（請求項１６）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるユーザ端末に搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、ワクチンセンタとの通信を行わせる通信プロセスと、ワクチンセンタから、該ウィルス検出ソフトを呼出して、ディジタルコンテンツがコンピュータウィルスに感染しているか否かを判定するウィルス検出プロセスと、ウィルス検出プロセスにおいて、コンピュータウィルスに感染している場合に、ワクチンセンタからウィルス除去ソフトを呼び出して、ディジタルコンテンツのコンピュータウィルスを除去するウィルス除去プロセスとを少なくとも有する。

【００２２】本発明（請求項１７）は、ディジタルコンテンツに関するライセンス使用条件書に、コンピュータウィルスの検出結果や除去結果であるウィルス検出日時、ウィルス検出ソフト名、ウィルスの有無、感染したコンピュータウィルスの種類、ウィルス除去日時の何れかを含む履歴データであるウィルス混入状況履歴データを記憶手段に書込むウィルス混入状況書込プロセスと、ウィルス混入状況履歴データをワクチンセンタに送信させるウィルス混入状況データ送信プロセスとをさらに有する。

【００２３】本発明（請求項１８）は、使用端末名、端末使用時間、使用コンテンツ名の何れかを含むユーザ端末環境データを抽出するユーザ端末環境データ抽出プロセスと、ユーザ端末環境データを記憶手段に記憶させるユーザ端末環境データ格納プロセスと、ユーザ端末環境データをワクチンセンタに送信させる環境データ送信プロセスとを更に有する。

【００２４】本発明（請求項１９）は、ユーザ端末におけるアプリケーションソフトウェアを含むディジタルコンテンツの使用許諾を管理するライセンス管理システム上でウィルスを検出し、ライセンスを管理するためのウィルス検出付ライセンス管理システムにおけるワクチンセンタに搭載されるウィルス検出付ライセンス管理プログラムを格納した記憶媒体であって、保持しているウィルス検出ソフトをユーザ端末の要求に基づいて送信させるウィルス検出ソフト送信プロセスと、保持しているウィルス除去ソフトをユーザ端末の要求に基づいて送信するウィルス除去ソフト送信プロセスとを有する。

【００２５】本発明（請求項２０）は、ユーザ端末から送信されたウィルス混入状況履歴データを記憶手段に格納するウィルス混入状況データ格納プロセスを更に有す

る。本発明（請求項２１）は、ユーザ端末から送信されるユーザ端末環境データを記憶手段に格納するユーザ端末環境データ格納プロセスを更に有する。上記のように、ユーザ端末がネットワークを介して接続されているワクチンセンタにウィルス検出ソフトやウィルス除去ソフトを用意しておき、ユーザ端末側でコンピュータウィルスの検出及び除去を行う際に、ワクチンセンタからソフトを取り出して、ウィルスの検出や、ウィルスの除去を行うことが可能となる。

【００２６】また、ユーザ端末のコンピュータウィルス混入状況の履歴を保持することにより、ワクチンセンタでは、ユーザ端末におけるウィルス混入の状況を把握することが可能となる。さらに、ユーザ端末のソフトウェアやハードウェアを含めた環境情報をワクチンセンタで把握することにより、前述のコンピュータウィルス混入状況と合わせてウィルス感染の端末の特定を可能とする。

【００２７】上記のように、従来は、コンピュータウィルス除去ソフトは、製品化された時点でコンピュータウィルスのデータベースを組み込むため、ユーザが購入した時点では、最新のコンピュータウィルスに対応しないが、本発明では、ユーザ端末において、ウィルス除去ソフトであるアンチウィルス除去ソフトを有するワクチンセンタと通信し、ウィルス検出ソフト、ウィルス除去ソフト、ウィルス混入状況履歴データ、ユーザ端末環境データを送受信することにより、最新のコンピュータウィルスに対応する。

【００２８】

【発明の実施の形態】図３は、本発明のウィルス検出付ライセンス管理システムの概要を示す。同図に示すシステムは、ユーザ端末２０００、最新のウィルス検出ソフト（ワクチンソフト）及びウィルス除去ソフト（アンチウィルスソフト）を有するワクチンセンタ３０００、ライセンス管理センタ４０００から構成される。

【００２９】ユーザ端末２０００は、アプリケーションソフトウェア２１００、受信部２２００及びウィルス検出・管理装置１０００から構成される。ウィルス検出・管理装置１０００は、ワクチンセンタ３０００との間でウィルスソフト、ウィルス除去ソフトを送受信することにより、アプリケーションソフトウェア２０００内のディジタルコンピュータがコンピュータウィルスに感染しているか否かを検出し、感染しているならば、当該コンピュータウィルスを除去する。

【００３０】また、ウィルス検出・管理装置１０００は、ワクチンセンタ３０００との通信によって、ウィルス混入状況データ、ユーザ端末環境データを送受信し、ウィルス混入状況やユーザ端末のソフトウェア、ハードウェアの使用環境を管理することで、ウィルス混入状況やウィルス感染端末状況からコンピュータウィルス感染の予防を実現することが可能である。

【００３１】ウィルス検出・管理装置１０００とワクチンセンタ３０００との間では、ウィルス検出ソフト、ウィルス除去ソフト、ウィルス混入状況データ、ユーザ端末環境データを送受信している。ウィルス検出・管理装置１０００でコンピュータウィルスに感染しているか否かを検出する際には、ウィルス検出ソフトであるワクチンソフトを格納するワクチンセンタ３０００と通信し、ウィルス検出ソフトを受け取って、ディジタルコンピュータがコンピュータウィルスに感染しているか否かを検出する。感染しているならば、ウィルス除去ソフトであるアンチウィルスソフトを格納するワクチンセンタ３０００から検出結果に該当するウィルス除去ソフトを呼び出す。また、ディジタルコンテンツ２１２０に関するライセンス使用条件書２１１０からは、ウィルス混入状況データをワクチンセンタ３０００に送信する。

【００３２】さらに、ライセンス管理センタ４０００は、アプリケーションソフトウェアデータベース４１００と顧客データベース４２００を有し、ワクチン管理センタ３０００に格納されているウィルス混入状況履歴データとユーザ端末環境履歴データからウィルス検出ソフトとウィルス除去ソフトの使用料を算出する。具体的には、ウィルス混入状況履歴データからユーザ端末２０００でウィスル検出ソフトやウィルス除去ソフトをどのぐらい使用したかの使用回数や使用時間等を計算する。

【００３３】図４は、本発明のユーザ端末の構成を示す。当該ユーザ端末２０００には、モニタ、キーボード、マウス等が接続されているものとする。なお、以下では、端末ソフトをユーザ端末として扱うものとし、モニタ、キーボード、マウス等は、ユーザ端末内のインタフェースを介して端末ソフトとやりとりされるものとする。

【００３４】同図に示すユーザ端末２０００は、ライセンス使用条件書２１１０、プログラムまたは文書等を含むディタルコンテンツ２１２０を有するアプリケーションソフトウェア２１００と、ウィルス検出・管理装置１０００を有する。ウィルス検出・管理装置１０００は、ウィルス検出処理部１１００、ウィルス除去処理部１２００、履歴データ管理処理部１３００、ユーザ端末環境抽出部１４００、記憶部１５００、通信処理部１６００及び制御部１７００から構成される。

【００３５】ウィルス検出処理部１１００は、記憶部１５００のウィルス検出ソフトを取り出し、アプリケーションソフトウェア２１００のディジタルコンテンツ２１２０がウィルス感染されているか否かを検出し、検出結果、検出ソフト名、検出日時等を記憶部１５００に格納する。ウィスル除去処理部１２００は、記憶部１５００のウィルス除去ソフトを取り出し、ディジタルコンテンツ２１２０等のウィルス除去を行い、ウィルス除去日時、除去結果、除去ソフト名、バージョン情報等を記憶部１５００に格納する。

【００３６】履歴データ管理処理部１３００は、記憶部１５００のウィルス混入状況履歴データをライセンス使用条件書に書き込む。ユーザ端末環境抽出部１４００は、ハードウェア、ソフトウェアの使用状況であるユーザ端末環境データを抽出し、記憶部１５００に格納する。記憶部１５００は、図５に示す構成を有する。記憶部１５００は、ウィルス検出ソフト、データ更新日時、ソフト番号等から構成されるウィルス検出ソフト記憶部１５１０、ウィルス除去ソフト、データ更新日時、ソフト番号等から構成されるウィルス除去ソフト記憶部１５２０、ウィルス検出日時、ウィルス感染の有無、検出ソフト名（バージョンを含む）、感染ウィルスの種類、ウィルス除去日時、除去ソフト名（バージョンを含む）等から構成されるウィルス混入状況履歴データ記憶部１５３０、及びコンピュータの種類、使用時間、使用ソフト等からなるユーザ端末環境データ記憶部１５４０から構成される。

【００３７】記憶部１５００は、ウィルス検出ソフト、ウィルス除去ソフトを、通信処理部１６００を介してワクチンセンタ３０００に取得要求を発行して取得し、それぞれウィルス検出ソフト記憶部１５１０及びウィルス除去記憶部１５２０に格納する。また、ウィルス混入状況履歴データ記憶部１５３０は、履歴データ管理処理部１３００からウィルス混入状況データを取得して格納する。ユーザ端末環境履歴データ記憶部１５４０は、ユーザ端末環境抽出部１４００からユーザ端末その時点における環境データを取得して格納する。

【００３８】通信制御部１６００は、制御部１７００の指令に基づいてワクチンセンタ３０００との通信を行い、ウィルス検出ソフト、ウィルス除去ソフトの要求・受信及び、ウィルス混入状況データ及びユーザ端末環境データの送信を行う。制御部１７００は、上記の各構成要素を制御する。

【００３９】

【実施例】以下、図面と共に本発明の実施例を説明する。まず、ワクチンセンタ３００には、最新の複数のウィルス検出ソフト、ウィルス除去ソフト（アンチウィルスソフト）、ウィルス混入状況履歴データ及びユーザ端末環境履歴データが格納されているものとする。

【００４０】次に、上記の構成における動作説明する。図６は、本発明の一実施例のウィルス検出・管理動作のシーケンスチャートである。

ステップ１０１）　まず、ユーザがユーザ端末において、アプリケーションソフトウェア２１００についてウィルスチェックを行いたい場合に、ユーザは、ウィルス検出・管理装置１０００を起動する。

【００４１】ステップ１０２）　この結果、制御部１７００の指令によって、通信処理部１６００は、ワクチンセンタ３０００と通信し、ウィルス検出ソフトを要求する。

ステップ１０３）　ワクチンセンタ３０００は、ユーザ端末２０００から要求されたウィルス検出ソフトを読み出して、ユーザ端末２０００に送信する。

ステップ１０４）　ユーザ端末２０００は、ウィルス検出ソフトをワクチンセンタ３０００から受信し、記憶部１５００のウィルス検出ソフト記憶部１５１０に格納する。

【００４２】ステップ１０５）　ユーザ端末２０００は、制御部１７００の指令によって、ウィルス検出処理部１１００は、記憶部１５００のウィルス検出ソフト記憶部１５１０に格納されているウィルス検出ソフトを取り出し、アプリケーションソフトウェア２１００がウィルス感染されているか否かを検出し、ウィルス検出日時や検出結果や検出ソフト名、バージョン情報等を記憶部１５００のウィルス混入状況履歴データ記憶部１５３０に格納する。

【００４３】ステップ１０６）　ステップ１０５において、ウィルスに感染していることが検出された場合には、ユーザからの指示または、自動的に制御部１７００の指令によって、通信処理部１６００は、ワクチンセンタ３０００と通信し、ウィルス除去ソフトを呼出す。

ステップ１０７）　ワクチンセンタ３０００は、要求されたウィルス除去ソフトを読み出して、ユーザ端末２０００に送信する。

【００４４】ステップ１０８）　ユーザ端末２０００は、記憶部１５００のウィルス除去ソフト記憶部１５２０に格納する。

ステップ１０９）　ユーザ端末２０００は、制御部１７００の指令によって、ウィルス除去処理部１２００は、記憶部１５００のウィルス除去ソフト記憶部１５２０に格納されているウィルス除去ソフトを取り出し、ディジタルコンテンツ２２００等のウィルス除去を行い、ウィルス除去日時や除去結果や除去ソフト名、バージョン情報等を記憶部１５００のウィルス混入状況履歴データ記憶部１５３０に格納する。

【００４５】ステップ１１０）　制御部１７００の指令によって、履歴データ管理処理部１３００は、ウィルス混入状況履歴データ記憶部１５３０に格納されているウィルス混入状況履歴データをライセンス使用条件書２１００に書き込む。

ステップ１１１）　制御部１７００の指令によって、通信処理部１６００は、記憶部１５００のウィルス混入状況データ記憶部１５３０に格納されているウィルス混入状況データを取り出し、ワクチンセンタ３０００に送信する。

【００４６】ステップ１１２）　ワクチンセンタ３０００は、ユーザ端末２０００から受信したウィルス混入状況データをウィルス混入状況履歴データに書き込む。

ステップ１１３）　ユーザ端末２０００は、制御部１７００の指令によって、ユーザ端末環境抽出部１４００

は、ハードウェア、ソフトウェア使用状況であるユーザ端末環境データを抽出し、記憶部１５００のユーザ端末環境データ１５４０に格納する。

【００４７】ステップ１１４）　また、制御部１７００の指令によって、通信処理部１６００は、記憶部１５００のユーザ端末環境データ１５４０に格納されているユーザ端末環境データを取り出し、ワクチンセンタ３０００に送信する。

ステップ１１５）　ワクチンセンタ３０００は、ユーザ端末２０００から受信したユーザ端末環境データをユーザ端末環境履歴データに書き込む。

【００４８】また、上記の実施例では、図３～図５の構成に基づいて説明したが、この例に限定されることなく、ユーザ端末及びワクチンセンタの各構成要素をプログラムとして構築し、ユーザ端末に接続されるディスク装置や、ワクチンセンタに接続されるディスク装置や、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより容易に本発明を実現することが可能である。

【００４９】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【００５０】

【発明の効果】上述のように、本発明によれば以下のような効果を奏する。第１には、ワクチンセンタ側に常に新しいウィルス検出ソフトを用意しておき、ユーザ端末に送信する構成をとることにより、コンピュータウィルスを検出することができる。

【００５１】第２には、ワクチンセンタ側に常に新しいウィルス除去ソフトを用意しておき、ユーザ端末で最新のウィルス除去ソフトを呼び出す構成をとることにより、コンピュータウィルスを迅速に除去できる。第３には、ディジタルコンテンツに関するライセンス使用条件書に記載されたウィルス混入状況履歴データを管理し、ウィルス混入状況履歴データをワクチンセンタに送信する構成をとることにより、コンピュータウィルスの混入状況を把握できることから、ウィルス伝搬状況を把握することができる。

【００５２】第４には、ユーザ端末環境を抽出し、ワクチンセンタに送信する構成をとることにより、コンピュータウィルスに感染されたユーザ端末環境データの履歴をとることによって、そのウィルス感染端末のソフトウェアとハードウェアの使用環境や設置場所を特定できるため、コンピュータウィルス感染対策を立てやすくなる。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

【図３】本発明のウィルス検出付ライセンス管理システムの概要を示す図である。

【図４】本発明のユーザ端末の構成図である。

【図５】本発明の記憶部の構成図である。

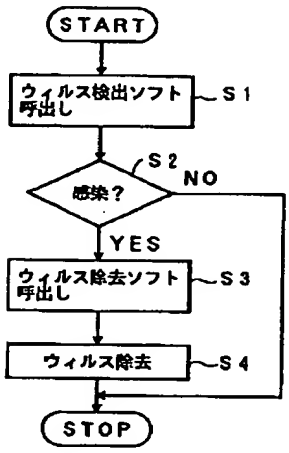
【図６】本発明の一実施例のウィルス検出・管理動作のシーケンスチャートである。

【符号の説明】

１０　ワクチンセンタ
１１　ウィルス検出ソフト保持手段
１２　ウィルス除去ソフト保持手段
２０　ユーザ端末
２１　通信手段
２２　ウィルス検出手段
２３　ウィルス除去手段
１０００　ウィルス検出・管理装置
１１００　ウィルス検出処理部
１２００　ウィルス除去処理部
１３００　履歴データ管理処理部
１４００　ユーザ端末環境抽出部
１５００　記憶部
１５１０　ウィルス検出ソフト記憶部
１５２０　ウィルス除去ソフト記憶部
１５３０　ウィルス混入状況履歴データ記憶部
１５４０　ユーザ端末環境データ記憶部
１６００　通信処理部
１７００　制御部
２０００　ユーザ端末（ユーザ端末ソフト）
２１００　アプリケーションソフトウェア
２１１０　ライセンス使用条件書
２１２０　ディジタルコンテンツ
２２００　受信部
３０００　ワクチンセンタ
４０００　ライセンス管理センタ

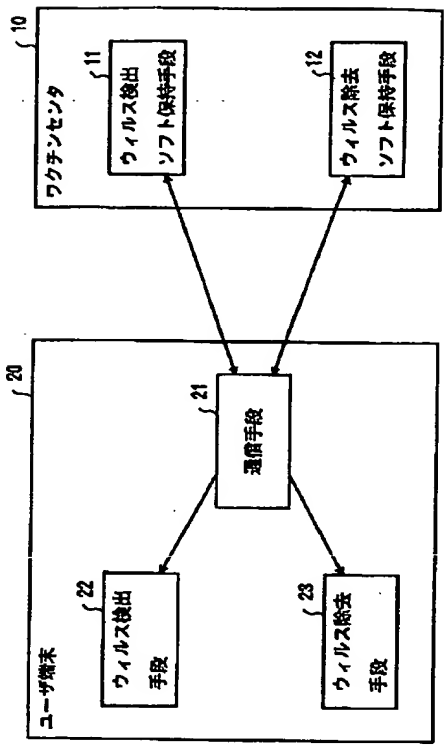
【図１】

本発明の原理を説明するための図



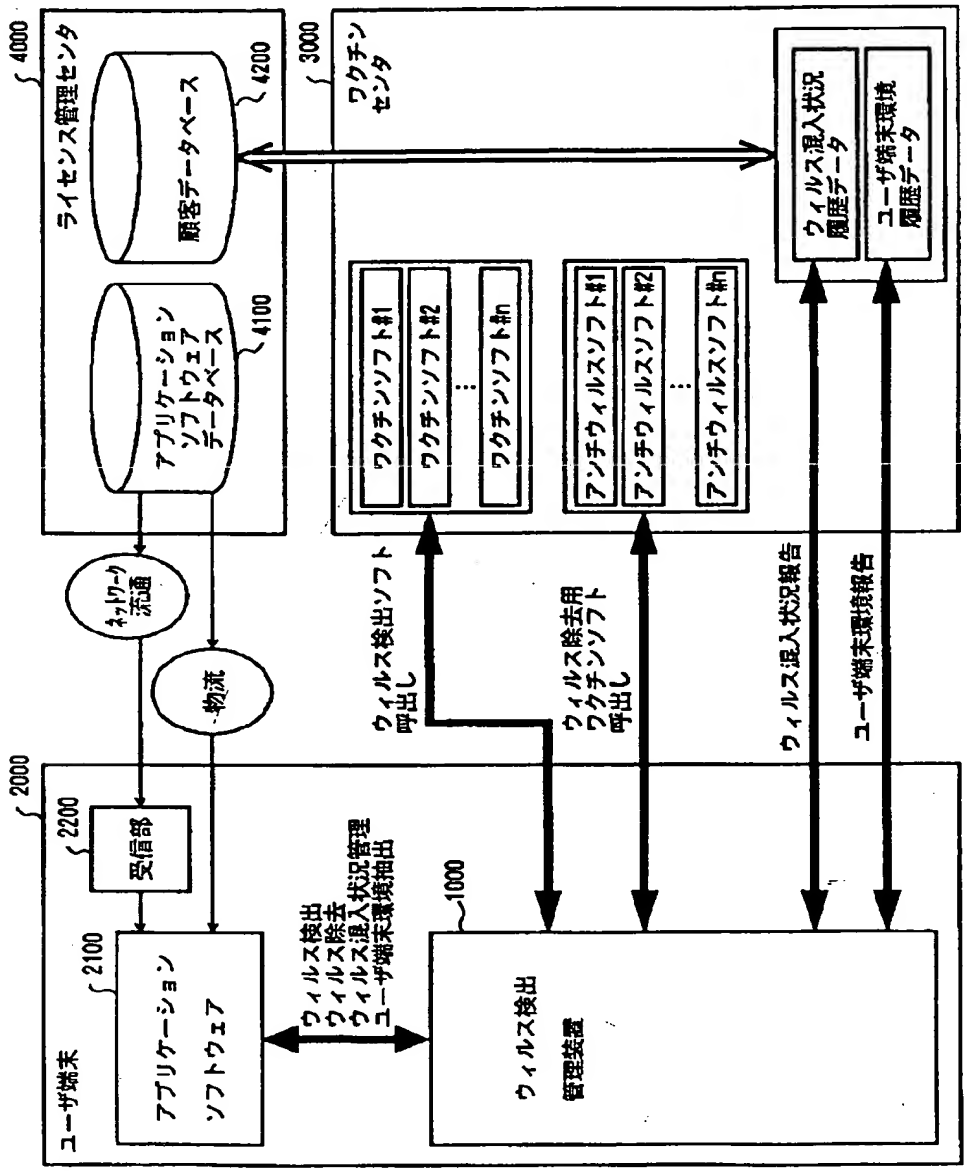
【図２】

本発明の原理構成図



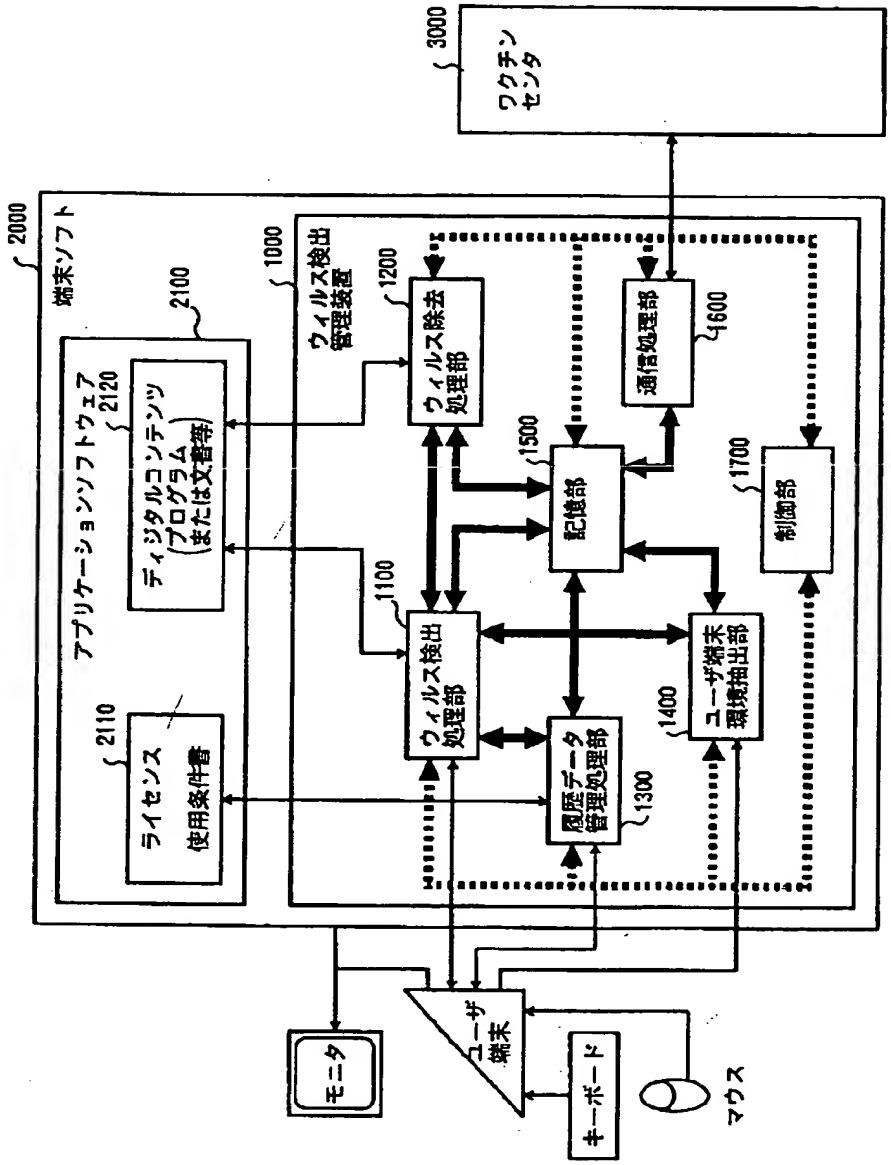
【図３】

本発明のウィルス検出付ライセンス管理システムの概要を示す図



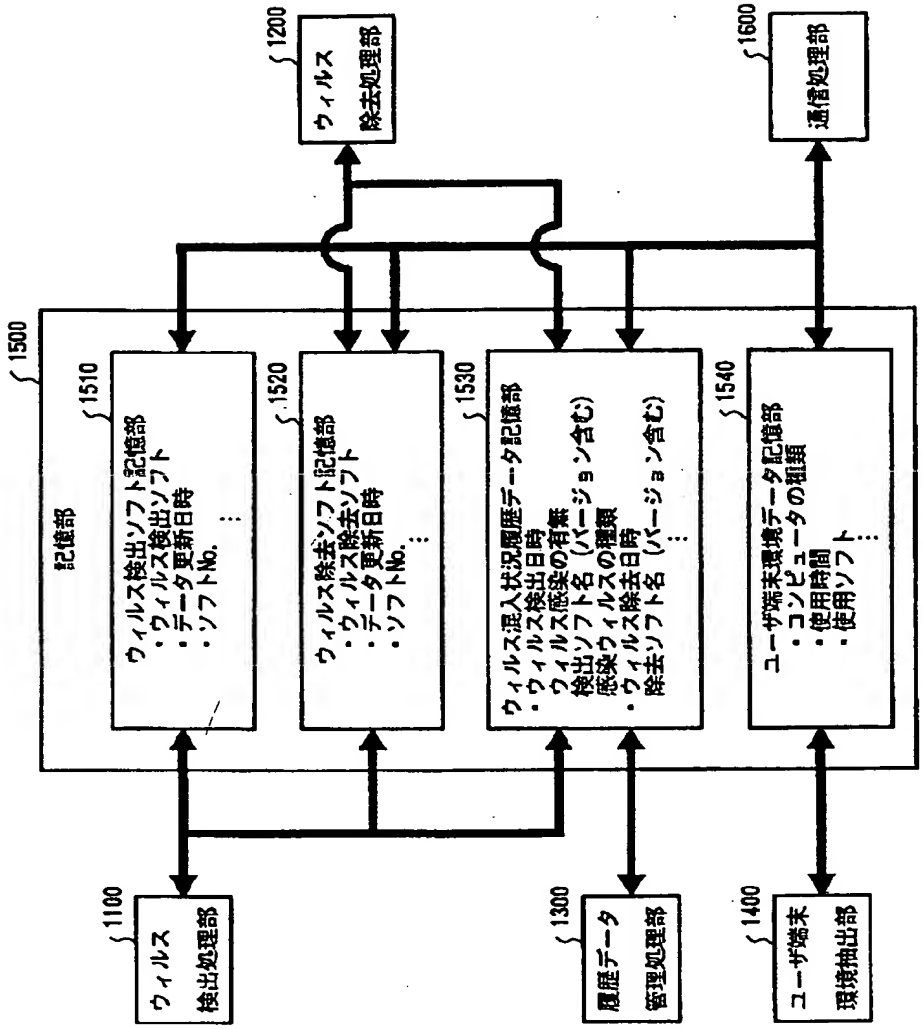
【図４】

本発明のユーザ端末の構成図



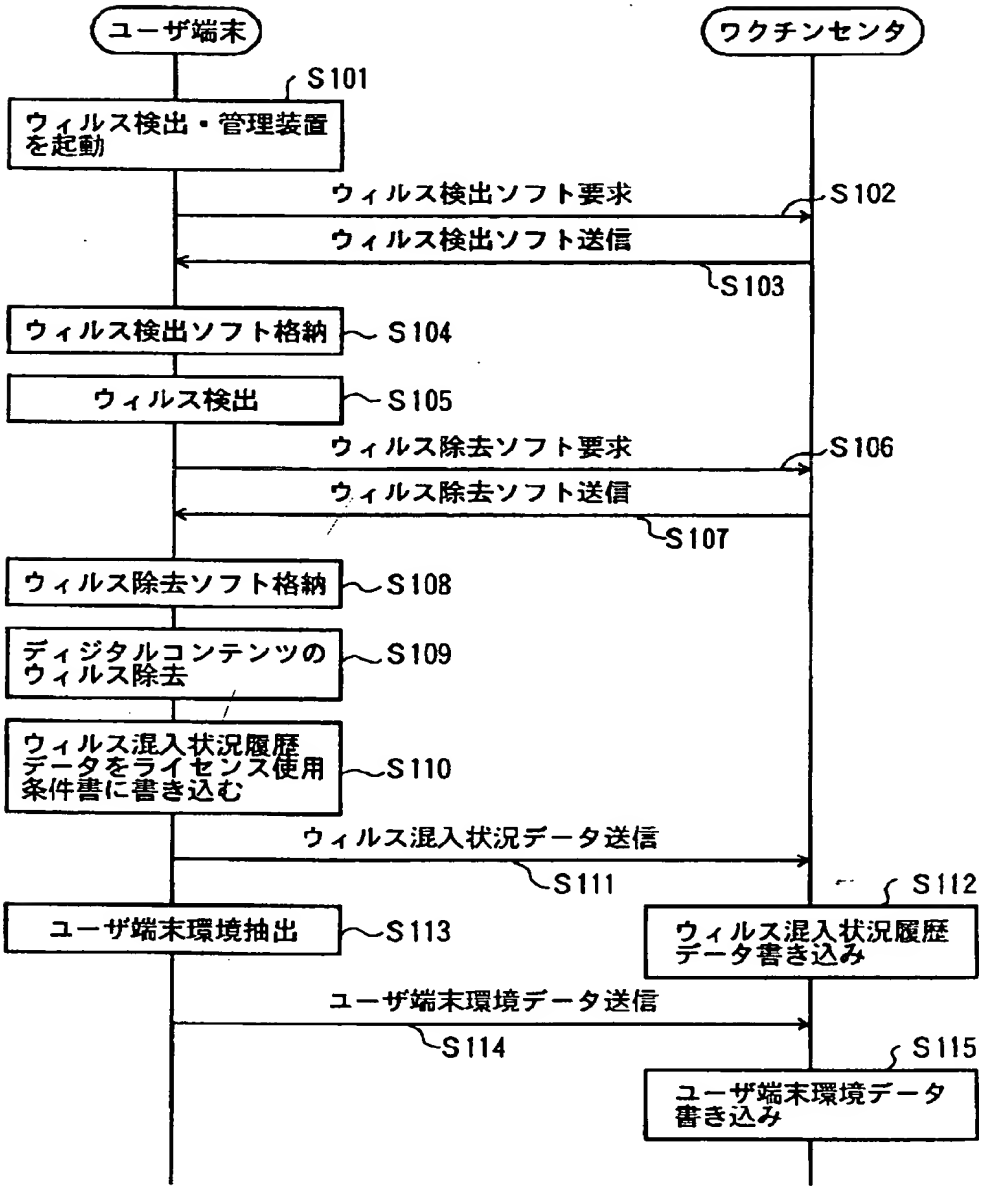
【図５】

本発明の記憶部の構成図



【図６】

本発明の一実施例のウィルス検出・管理動作のシーケンスチャート



フロントページの続き

(72)発明者　印牧　直文
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　若井　卓実
東京都中央区日本橋箱崎町24－１　エスビーネットワークス株式会社内

(72)発明者　菅野　優紀
東京都中央区日本橋箱崎町24－１　エスビ
ーネットワークス株式会社内

Ｆターム(参考)　5B076 FD08